# ANALISA GENERALISASI RULES MENGGUNAKAN SNORT IDS

SKRIPSI

Diajukan Untuk Memenuhi Persyaratan

Dalam Memperoleh Gelar Sarjana Komputer

Jurusan Teknik Informatika


Disusun Oleh :

WISNU HADI SUWANDONO

NPM. 0934010144



JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAWA TIMUR


2013

# ANALISA GENERALISASI RULES MENGGUNAKAN SNORT IDS

SKRIPSI


Disusun Oleh :

WISNU HADI SUWANDONO

NPM. 0934010144

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2013

# ANALISA GENERALISASI RULES MENGGUNAKAN SNORT IDS

SKRIPSI

Diajukan Untuk Memenuhi Persyaratan

Dalam Memperoleh Gelar Sarjana Komputer

Jurusan Teknik Informatika


Disusun Oleh :

WISNU HADI SUWANDONO

NPM. 0934010144



JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAWA TIMUR


2013

# LEMBAR PENGESAHAN

ANALISA GENERALISASI RULES MENGGUNAKAN

SNORT IDS

Disusun Oleh :

Wisnu Hadi Suwandono

0934010144

Telah disetujui mengikuti Ujian Negara Lisan

Periode III Tahun Akademik 2013

Menyetujui,

| Pembimbing Utama | Pembimbing Pendamping |
| --- | --- |
| I Made Suartana, S.Kom, M.Kom. | Kafi Ramadhani B, S.Kom. |
| | NPT. 3 8904 13 0345 1 |

Mengetahui,

Ketua Program Studi Teknik Informatika

Fakultas Teknologi Industri

Universitas Pembangunan Nasional “Veteran” Jawa Timur

Dr. Ir. Ni Ketut Sari, M.T.

NIP. 19650731 199203 2 001

# SKRIPSI

ANALISA GENERALISASI RULES MENGGUNAKAN SNORT IDS

Disusun Oleh :
Wisnu Hadi Suwandono
0934010144

Telah dipertahankan dan di terima oleh Tim Penguji Lisan
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional “Veteran” Jawa Timur
Pada tanggal : 20 Desember 2013

Pembimbing :
1.

I Made Suartana, S.Kom., M.Kom.

2.

Kafi Ramadhani B, S.Kom.
NPT. 3 8904 13 0345 1

Tim Penguji :
1.

I Gede Susrama, S.T., M.Kom.
NPT. 3 7006 060 211 1

2.

Fetty Tri Anggraeny, S.Kom., M.Kom.
NPT. 3 8202 060 208 1

3.

Henni Endah Wahanani, S.Kom., M.Kom.
NPT. 3 7809 130 348 1

Mengetahui,
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional “Veteran” Jawa Timur

Ir. Sutiyono, M.T.
NIP. 19600713 198703 1 001

# KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Syukur Alhamdulillah atas segala limpahan karunia dan kasih sayang Allah SWT, sehingga dengan segala keterbatasan waktu, tenaga, dan pikiran yang dimiliki oleh penulis, akhirnya skripsi yang berjudul "ANALISA GENERALISASI RULES MENGGUNAKAN SNORT IDS" dapat terselesaikan sesuai dengan waktu yang telah ditetapkan.

Melalui Skripsi ini, penulis merasa mendapat kesempatan besar untuk memperdalam ilmu pengetahuan yang diperoleh selama di perkuliahan, terutama dengan implementasi Teknologi Informasi dalam kehidupan sehari-hari. Namun demikian penulis menyadari bahwa Skripsi ini masih memiliki banyak kelemahan dan kekurangan. Oleh karena itu, kritik dan saran yang bersifat membangun sangatlah diharapkan dari berbagai pihak agar Skripsi ini bisa lebih baik lagi, sehingga dapat memberikan manfaat bagi semua pihak yang membutuhkannya.

Pada penyusunan Skripsi ini, banyak pihak yang telah memberikan bantuan baik materiil maupun spiritual ini, sehingga pada kesempatan ini penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. ALLAH SWT dan RASUL-Nya. Alhamdulillah atas segala kelancaran dan kemudahan yang selalu engkau limpahkan kepada penulis.
2. Ibu Dr.Ir. Ni Ketut Sari,M.T. selaku ketua jurusan Teknik Informatika, UPN "Veteran" Jawa Timur.

3. Bapak I Made Suartana, S.Kom, M.Kom dan Bapak Kafi Ramadhani Borud, S.Kom. selaku dosen pembimbing . Terimakasih banyak telah sabar membimbing dan memberi saran yang sangat bermanfaat kepada penulis.
4. Teman-teman TFC'09, terimakasih selalu meramaikan dan memberi hiburan disaat dalam kejenuhan.
5. For My Beloved Syilvia Nur Aini Terima kasih atas supportnya,waktu dan doanya.
6. The last and the best, thanks to my beloved family Ibu, Alm.Ayah, Tante ku yang selalu menjadi motivasi untuk cepat lulus kuliah.

Serta pihak-pihak lain yang ikut memberikan informasi dan data-data di dalam menyelesaikan laporan Skripsi ini, penulis mengucapkan terima kasih.

Akhir kata penulis harap agar Skripsi yang disusun sesuai dengan kemampuan dan pengetahuan yang sangat terbatas ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Wassalamu'alaikum Wr. Wb

Surabaya, Desember 2013

Penulis

# DAFTAR ISI

Halaman

DOSEN PEMBIMBING I : I MADE SUARTANA, S.Kom, M.Kom
DOSEN PEMBIMBING II : KAFI RAMADHANI BORUD, S.Kom
PENYUSUN : WISNU HADI SUWANDONO

# ABSTRAK

Perkembangan teknologi jaringan komputer semakin berkembang, seiring dengan itu semakin banyak terjadi serangan pada jaringan komputer. Serangan yang paling sering terjadi adalah Denial of Service (DOS attack), serangan SYN Flood salah satunya, dimana serangan ini bisa berakibat fatal pada target apabila dilakukan secara terus menerus.

Salah satu pencegahan yang umum dilakukan adalah dengan menambahkan Intrusion Detection System (IDS) yang memberikan lapisan keamanan pada sistem komputer dan jaringan. IDS bertanggung jawab untuk mendeteksi aktivitas jaringan yang mencurigakan atau tidak dapat diterima pada sistem yang nantinya akan memberi peringatan (alert) kepada administrator jaringan. Snort merupakan salah satu IDS yang populer digunakan dan secara aktif mengembangkan open source yang menggunakan satu set Signature yang dikenal dengan Snort Rules. Mencocokan pola atau Signature adalah metode yang digunakan pada IDS untuk mendeteksi serangan yang kemudian akan menghasilkan alert. Terkadang terdapat beberapa kelemahan dari alert yang dihasilkan apakah alert menunjukan serangan yang sebenarnya terjadi (true alert) atau menunjukan serangan yang bukan sebenarnya (false alert).

Dengan menambahkan generalisasi sederhana (removing dan inverting) pada Snort Rules diharapkan IDS dapat menghasilkan alert yang lebih bervariasi dan mampu mendeteksi dengan benar serangan yang terjadi khususnya disini serangan SYN Flood. Terbukti dengan melakukan generalisasi sederhana mampu meningkatkan akurasi dari alert yang dihasilkan dengan nilai prioritas yang lebih kecil daripada Snort Rules standart.

Keyword : Deteksi anomali, Intrusioon Detection System, Snort, Snort Rules, Generalisasi sederhana

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Penggunaan jaringan komputer saat ini semakin meluas tidak hanya digunakan untuk perorangan tetapi juga dibutuhkan baik untuk organisasi, instansi ataupun perusahaan. dikarenakan kemudahan untuk saling bertukar data dan informasi. Terkadang data atau informasi bersifat pribadi dan sangat penting sehingga diperlukan suatu pengaman tertentu agar tidak jatuh ke pihak yang tidak bersangkutan. Keamanan jaringan merupakan hal yang harus diperhatikan dalam membangun suatu jaringan komputer untuk menghindari serangan-serangan dari pihak yang merugikan. saat ini banyak bermunculan cara dan teknik yang dilakukan penyusup untuk masuk kedalam suatu jaringan komputer. Hal itu diperlukan cara pencegahan dengan melakukan pendeteksian serangan secara awal sehingga meminimalkan resiko dan kemudian dapat melakukan pencegahan yang tepat. Salah satu contohnya menggunakan Sistem Deteksi Intrusi atau Intrusion Detection System (IDS) pada jaringan tersebut. Menurut Onno Purbo (2010), IDS merupakan usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal cracker) atau seorang user yang sah tetapi menyalahgunakan (abuse) sumber daya sistem.

IDS bertanggung jawab untuk mendeteksi tindakan atau hal, sistem yang tidak dapat diterima dan aktivitas jaringan yang mencurigakan. Kemudian IDS

akan memberi peringatan (Alert) kepada Administrator bahwa telah terjadi serangan didalam jaringan tersebut. Kebanyakan IDS menggunakan satu set tanda tangan (Signature) yang mendefinisikan bahwa telah terjadi tindakan atau hal yang mencurigakan dalam network traffic. Salah satu serangan yang umum dilakukan adalah serangan SynFlood, SynFlood merupakan serangan dengan cara mengirimkan paket SYN sebanyak mungkin ke target tanpa mengirimkan paket ACK,sehingga target tidak dapat lagi memberikan layanan atau menerima request dari client lain. Serangan seperti ini biasanya dilakukan pada layanan-layanan terbuka seperti layanan web/HTTP, FTP. Apabila serangan ini dilakukan secara terus menerus maka target akan bisa mengalami hang atau crash.Snort merupakan salah satu IDS populeryang banyak digunakan untuk mendeteksi suatu paket jaringan dan Snort merupakanopen sourcyang aktif melakukan pengembangkan menggunakan suatuset tanda tangan yang dikenal sebagai aturan Snort (Snort Rule).

Maka dari itu penulis melakukan Generalisasi Rule Menggunakan SNORT IDS (Intrusion Detection System)untuk mengidentifikasi cara di mana Snort dapat dikembangkan lebih lanjut dengan Generalisasi Ruleagar dapat mendeteksi serangan SynFlood atau bahkan serangan-serangan baru.

## 1.2 Rumusan Masalah

Berdasarkan dari uraian latar belakang di atas maka dapat dirumuskan suatu permasalahan.

1. Bagaimana mendeteksi serangan atau intrusi yang akan terjadi menggunakan Snort IDS.

2. Bagaimana melakukan pola Rule Generalisasi Snort pada Rule standart untuk dapat mengidentifikasi serangan SynFlood atau bahkan serangan baru yang terjadi didalam network traffic.
3. Bagaimana menampilkan alert hasil dari generalisasi rule dan melakukan analisa.

## 1.3 Batasan Masalah

Dalam melakukan Generalisasi Rule Menggunakan SNORT IDS (Intrusion Detection System), mempunyai batasan masalah sebagai berikut:

1. Metode Generalisasi yang digunakan adalah generalisasi sederhana yaitu generalisasi invert (menghilangkan salah satu parameter) dan generalisasi content (melakukan pembalikan pada nilai atau isi dari salah satu parameter).
2. Pendeteksian serangan terbatas pada serangan Denial of Service attacks, SynFlood attack, IP dan Port scanning.
3. Data Paket Jaringan yang digunakan adalah data paket yang berhasil di-log oleh SNORT.
4. Pada penelitian tugas akhir ini parameter rules snort yang digunakan untuk generalisasi rule adalah :
    a) Depth
    b) Offset
    c) Content

## 1.4 Tujuan

Tujuan dari Tugas Akhir ini adalah :

1. Mengerti dan memahami jenis-jenis serangan pada serangan Denial of Service attacks, SynFlood attack, IP dan Port scanning.
2. Memahami dan mampu mengaplikasikan Generalisasi Rule Menggunakan SNORT IDS (Intrusion Detection System)untuk mengidentifikasi serangan SynFlood dan serangan-serangan baru.

## 1.5 Manfaat

Manfaat dari Tugas Akhir ini adalah :

1. Meminimalisir adanya kesalahan dan celah keamanan dari sebuah sistem jaringan komputer.
2. Meminimalisir kesalahan Alert yang dihasilkan dari IDS.
3. Mengamankan jaringan komputer berbasis client-server menggunakan debian server agar dapat melakukan pencegahan yang sesuai bedasarkan serangan yang terjadi.

## 1.6 Metodologi Penelitian

Langkah-langkah yang dilakukan untuk pembuatan Tugas Akhir ini dibagi menjadi beberapa tahapan, sebagai berikut:

a) Studi Literatur

Pada tahap ini dilakukan studi literatur terhadap konsep dan metode ysng akan digunakan dan pengumpulan data-data yang dibutuhkan.

b) Menetapkan definisi kebutuhan

Pada tahap ini dilakukan pendefinisian terhadap kemampuan perangkat lunak yang akan dirancang dan batasan-batasannya.

c) Perancangan Sistem

Pada tahap ini dilakukan Perancangan model jaringan, simulasi serangan, analisa kebutuhan sistem, penyediaan Hardware dan Software pendukung dan perancangan kerja sistem.

d) Implementasi Sistem

Pada tahap ini dilakukan pengimplementasian Instalasi, konfigurasi dan pengetesan kerja sistem.

e) Uji coba dan Analisa

Pada tahap ini dilakukan uji coba dan analisa terhadap sistem dengan melakukan penyerangan dan kemudian membandingkan hasil dari pendeteksian sistem.

f) Penyusunan Naskah Tugas Akhir

Pada tahap ini dilakukan penulisan naskah, dimana didalamnya menjelaskan teori yang dipergunakan serta penyusunan laporan.

## 1.7 Sistematika Penulisan

Sistematika penulisan Tugas Akhir (TA) ini akan membantu mengarahkan penulisan laporan agar tidak menyimpang dari batasan masalah yang dijadikan sebagai acuan atau kerangka penulisan dalam mencapai tujuan penulisan laporan Tugas Akhir (TA) sesuai dengan apa yang diharapkan. Tugas Akhir (TA) ini terbagi dalam V Bab, yaitu :

BAB I PENDAHULUAN

Pendahuluan ini berisi mengenai gambaran umum tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka ini berisi tentang gambaran umum objek pekerjaan pengertian - pengertian dasar dan teori - teori yang berhubungan dengan masalah yang akan di bahas dalam Tugas Akhir (TA) ini sebagai landasan bagi pemecahan yang di usulkan.

BAB III METODOLOGI PENELITIAN

Metodologi Penelitian ini berisi tentang perencanaan, analisa kebutuhan sistem dan perancangan sistem.

BAB IV HASIL DAN PEMBAHASAN

Hasil dan Pembahasan ini berisi tentang pembuatan sistem, hasil dan pembahasan mengenai pendeteksi serangan atau intrusi yang akan terjadi dan

pengenalan pola terhadap penyerangan menggunakan aturan generalisasi untuk meng-generalisasi Snort Rules agar dapat mendeteksi serangan baru

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan yang di peroleh dari hasil pengana-lisaan data dari bab-bab sebelumnya. Dimana berisi tentang saran-saran yang diharapkan dapat bermanfaat dan dapat membangun serta mengembangkan isi laporan tersebut sesuai dengan tujuan penulisan Laporan Tugas Akhir (TA).

LAMPIRAN

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembuatan laporan tugas akhir ini.